ANTI-MONEY LAUNDERING & MORTGAGE FRAUD COMPLIANCE PROGRAM

Version: 2.0 dated 08.2013

TABLE OF CONTENTS

1.0 PURPOSE AND SCOPE

It is the purpose of ResMac to support and fully comply with the anti-money laundering compliance program (the "Program") required of all mortgage lenders published by the Treasury Department under their authority granted by the Bank Secrecy Act, to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorists or criminal activity through the use of money laundering or any type of mortgage fraud.

Money laundering is generally defined as any act designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful (laundered) proceeds appear to be legitimate assets from legitimate sources. Mortgage Fraud is any act undertaken to encourage or induce a lender to make a loan, when the lender would likely have not made the loan had the true facts been known. Both of these actions are reportable under the Bank Secrecy Act, using a Suspicious Activity Report (SAR.)

The following Program applies to all ResMac Inc. (the "Company") locations and business, and implements procedures and policies to comply with the rules for non-bank residential mortgage companies pertaining to any loans ("loans") the Company makes and/or processes for the purpose of identifying, evaluating, recording and reporting suspicious activity in connection with mortgage lending, as appropriate and as required.

Suspicious activity refers to issues with or documentation related to all parties to the transaction, including identity issues, asset issues and any other activity of a suspicious nature in connection with prospective or actual business.

All ResMac employees must be aware of the Program, the Requirements and the responsibility they share to appropriately report suspicious activity.

2.0 APPLICABLE REGULATIONS AND GUIDANCE

Bank Secrecy Act (BSA)
12 U.S.C. 1829b, 12 U.S.C. 1951–1959, and 31 U.S.C. 5311–5314 and 5316–5332

- The BSA requires financial institutions to keep records and file reports that the Secretary of the Treasury determines ''have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism."

Anti-Money Laundering (AML) Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators
31 CFR Parts 1029.210 & 1029.300 Subpart C

- AML Program Minimum Requirements

(1) ResMac has incorporated these Policies and Procedures and Internal Controls based on the company's assessment of money laundering and terrorist financing risks associated with its products and services, and has developed this AML program to deal with the risks and reporting.

(2) ResMac has designated a compliance officer who will be responsible for ensuring that:
   i. The AML program is implemented effectively, including monitoring compliance by the company's agents and brokers with their obligations under the program;
   ii. The AML program is revised as necessary;
   iii. Appropriate persons are educated and trained in accordance with the training requirements under the rule.

(3) ResMac provides for on-going training of appropriate persons concerning their responsibilities under the program.

(4) ResMac provide for independent testing to monitor and maintain an adequate program, including periodic testing to determine compliance of the company's agents and brokers with their obligations under the program. The scope and frequency is commensurate with the risks posed by the company's products and services, and will be regularly evaluated and updated.

- Suspicious Activity Report Filing Requirements

A transaction requires reporting if it involves or aggregates funds or other assets of at least $5,000, and the non-bank mortgage lender knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

(1) Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;

(2) Is designed, whether through structuring or other means, to evade any requirements of this part or any other regulations promulgated under the Bank Secrecy Act, Public Law 91–508, as amended, codified at 12 U.S.C. 1829b, 12 U.S.C. 1951–1959, and 31 U.S.C. 5311–5314, 5316–5332;

(3) Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the loan or finance company knows of no reasonable explanation for the transaction after examining the

available facts, including the background and possible purpose of the transaction; or

(4) Involves use of the loan or finance company to facilitate criminal activity, including any type of misrepresentation which could induce a lender to make a loan, i.e., any type of activity that could be classified as 'mortgage fraud.'

3.0 PROGRAM AND GUIDELINES

Financial institutions are expected to understand, identify and assess their risks, take appropriate actions to mitigate them and allocate their resources efficiently by focusing on higher risk areas.

The Chief Compliance Officer will periodically conduct an assessment of company's risks and present that assessment to Senior Management for approval, and will continually assess the changing risks when new products and services are introduced, existing products and services change, higher-risk customers open accounts, or when ResMac, Inc. expands through mergers and/or acquisitions. In no case will the reassessment take place less frequently than every eighteen (18) months.

The risk assessment will include the following: and identification of risks, including risks by; 1) types of overall company business and their associated risks, 2) types of products and associated risks, 3) types of origination methods and channels and associated risks, and 4) geographic location.

After identifying the types of risks, the Compliance Officer shall assign a level to each risk by assessing the likelihood and frequency of the risk occurring, and assessing the severity of the risk if it were to occur.

The Compliance Officer will then work with each functional department, including but not limited to, funding, closing, underwriting, processing, origination (including third party originators), and accounting, to develop appropriate controls to address and mitigate the risks and incorporate the controls into their department's policies and procedures.

Each department head will then implement the controls developed and assess compliance with the controls annually at a minimum and report the results of such assessment to the Chief Compliance Officer.

Our policy covers multiple items that require verification of the customer, their assets, and the transactional characteristics, any of which could potentially be suspicious activities that require reporting to Compliance and evaluation and research by the Compliance Officer at a minimum. If items are resolved, these are only tracked but not reported. If unresolved, they must be reported to the appropriate authorities, who then complete their own research and pursue any issues independent of ResMac.

3.1 Customer Identification and Verification

We maintain a written Customer Identification Program (or CIP) so that we know our customers. We collect at minimum basic customer identification information from each potential applicant and utilize risk-based measures to verify the identity; we notify our customers that we require identification information and compare customer identification information with government-provided lists of suspected terrorists for all applicants. In addition we verify all parties to the transaction against various agency debarment lists as required. We confirm the true identity of our customers by using risk-based procedures to further verify and document the accuracy of the information we get about our customers during every step of processing a loan, including analyzing any inconsistencies in the information we obtain.

3.11 Required Customer Information

We will collect the following information for all customers: name; address, social security or other identification number; identification (usually driver's license or resident alien card) evidencing residence and bearing a photograph. We will refuse any loan in the event that a customer has not received a taxpayer identification number and cannot prove his/her identity satisfactorily.

Copies of identification are retained in the image system for each loan.

Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For an entity, other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

3.12 Notice to Customers

We will provide notice to applicants that ResMac requires information from them to verify their identities, as required by Federal law. We will give written notice to all applicants as part of the application disclosures. These are tested with our random and designated pre and post-closing QC, as well as verified at the time each loan is submitted to the operations center.

3.13 Following are some of the way to verify identity:

- Obtain copies of identification from each borrower (required)
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, employer or other source

- Checking references with financial institutions

3.14 Customers Who Refuse To Provide Information

- If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not continue processing business for that person. The Compliance Officer must be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-MSB).

3.15 If we are Unable to Verify Identity

If we are unable to positively identify a prospective borrower, we will:

- not do any business with that person, and
- The information should be referred to the Compliance Officer for further research and possible filing of a SAR.

3.2 Verification of all parties to the Office of Foreign Assets Control (OFAC) Lists

- As part of the processing of any loan application, we will determine whether a customer and/or any party to a loan transaction appears on any such list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators. We will follow all Federal directives issued in connection with such lists.
- Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.
- We will continue to comply with Treasury's OFAC rules prohibiting transactions with certain foreign countries or their nationals. Any positive matches to the list that are not clearly resolved must be referred to Compliance for further research. If we determine a customer, or someone with or for who the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and proceed according to OFAC requirements in reporting the person listed.
- We require verification of all customers and parties to the transaction to the LDP/GSA list as well as OFAC.

3.3 Detecting Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to the following items.

Any employee discovering anything unexplained during the taking of or processing applications MUST report these items directly to the Compliance Officer. Examples include:

:

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business),
- Customer is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or documents.
- The customer wishes to engage in a transaction that lacks business sense or is inconsistent with the customer's stated business.
- The information provided by the customer purporting to be a legitimate source for funds, is revealed to be false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person
- The customer has difficulty describing the nature of his or her business.
- The customer asks for exemptions from the Company's AML policies.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds. (unlikely we would see these)
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
- The customer has unexplained or sudden extensive money service activity, especially when they that had little or no previous activity, including large unexplained deposits showing on statements.
- The customer has inflows of funds or other assets well beyond the known income or resources of the customer.
- The customer has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer has financial activity with no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer requests that a transaction be processed to avoid the Company’s normal documentation requirements.
- The customer uses multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent purpose.

- Provided bank statements or paystubs appear suspicious or altered
- Any other unexplained discrepancy that appears could be a red flag

3.30 Responding to Red Flags and Suspicious Activity

When a member of the Company detects any red flag that upon further study cannot be resolved, he or she should immediately contact the Compliance Officer for direction. In many cases the issue may be able to be easily resolved, and processing of the loan can continue.

The Compliance Officer may ask for the employee's assistance [for example, asking them to contact customer for more information], depending upon the status of the loan process. Compliance may assume the research entirely, particularly on a closed or cancelled or denied loan.

Each employee is responsible for reporting suspicious items to Compliance officer (either via email or by utilizing the ***Suspicious Activity Reporting Form*** utilized under Forms on the ResMac website.) Managers and Employees have been notified that they are responsible for reporting any suspicious issues or items noted during the processing of loan applications. Reporting of any suspicious activity or issues is to be directed to compliance@resmac.us or directly to the Compliance Officer, jdelormier@resmac.us .

What happens if we cannot confirm or explain something?

If any identified suspected risk cannot be explained or resolved by the identified controls, then ResMac will decline the associated transaction and may file a Suspicious Activity Report (SAR). Because it is confidential, the person who originally noticed the issue or discrepancy will generally never know if a SAR has been filed.

4.0 RESPONSIBILITIES & COMPLIANCE OFFICER DESIGNATION

The ultimate authority and responsibility for this Program lies with Senior Management of ResMac.

Senior Management has delegated the following responsibilities to and designates Jeanne DeLormier as the Compliance Officer. The Compliance Officer is responsible for ensuring; i.) The Program is implemented effectively, including monitoring compliance by the company's agents and brokers with their obligations under the program; ii.) The AML program is updated as necessary; iii.) Appropriate persons are educated and trained in accordance with the training requirements under the rule; and iv., filing and retaining SAR records.

Each functional manager, in consultation with the Compliance Officer, is responsible for implementing the controls developed into their department's policies and procedures.

Senior Management further delegates all other responsibility for implementing, monitoring and maintaining this Program, including the assessment of risk, and development of policies and procedures to mitigate those risks, and the guidelines set forth herein to the Chief Compliance Officer who will report on processes and progress at least annually to Senior Management.

The Chief Compliance Officer will be responsible for reporting and retaining copies of the confidential SAR reporting. When warranted, the Compliance Officer will ensure Suspicious Activity Reports (e-Form TD F90-22.56) are filed with the Financial Crimes Enforcement Network (FinCEN). Only the Chief Compliance Officer, the Compliance Manager and the President shall have access to filed SARs in keeping with the restrictive nature of the program.

The entire program, including the policies and procedures developed to address and mitigate risks, will be assessed by the Chief Compliance Officer and Compliance Manager as directed by Senior Management at least annually. The Policy is posted on the internal website and accessible by all employees.

5.0 TRAINING

It is the responsibility of the Compliance Officer to ensure that all managers provide appropriate training for their employees, making sure they are aware of the objective of this Program and are trained on the procedures promulgated to implement this program and the guidelines set forth herein. Annual training will be provided by Compliance for each employee, tracking to ensure completed.

Training programs on Red Flags / Suspicious Activity Identification, as well as how to report suspected or confirmed issues, will be held periodically; updates on current issues and trends, as well as reminders on the program, will be issued to all employees at least quarterly via ResMac ReadMe announcements.

Information on potential violations and Red Flags is posted on the Internal ResMac website with restricted access for employees only. Employees are periodically reminded of the requirement for reporting. A form for any employee to utilize in reporting any suspicious activity for further investigation is on the internal Website under Forms.

6.0 MONITORING, RECORDKEEPING, & INFORMATION SHARING

The Compliance Manager or designee, which may include utilizing a third party company in conjunction with other quality control testing, at the direction of the Chief Compliance Officer, will periodically conduct such tests and submit such reports as necessary to document that the requirements outlined in this Program are being maintained and

followed. The Compliance Manager or their designee will report on compliance with the Program to ResMac's Chief Compliance Officer and the company President at least annually with updates whenever required.

Recordkeeping. All records under this Program, including supporting documentation behind the Suspicious Activity Report shall be maintained for a minimum of five (5) years from the date the loan transaction is funded or from when the Suspicious Activity Report is filed, whichever is later. The Chief Compliance Officer will ensure that all records are uploaded to a designated location for storage and retention. Information is considered restricted with access restricted to the President of ResMac, the Chief Compliance Officer, and the Compliance Manager.

Sharing Information We will respond to any FinCEN request about accounts or transactions by immediately searching our records to determine if we have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. The Compliances Officer is responsible for responses. We are required to search current transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form in a timely manner. If we search our records and do not uncover a matching account or transaction, then we will not reply as allowed under Section 314(a) of the PATRIOT Act.

We may also chose to respond to or share information regarding possible terrorist activities with other financial institutions, if allowed. We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, as required by Section 501 of the Gramm-Leach-Bliley Act. We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

7.0 FILING A FORM SAR

We will file Form SAR *OMB No. 1506-0065* for any activity (including deposits and transfers) conducted or attempted through our Company involving (or in the aggregate) $5,000 or more of funds or assets where we know, suspect, or have reason to suspect:

1) the transaction involves or appears to involve funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation,

2) The transaction is designed, whether through structuring or otherwise, to evade the any requirements of the BSA regulations,

3) the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or

4) The transaction involves the use of the Company to facilitate criminal activity., based on some other identified discrepancy or misrepresentation discovered in the file documents

We will not base our decision on whether to file a SAR solely on whether the transaction falls above a set threshold.

We will file a SAR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the appropriate government agency immediately and will file a SAR with FinCEN.

We will report suspicious transactions by completing a SAR and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR no later than 30 calendar days after the date of the initial detection/confirmation of the facts that constitute a basis for filing a SAR. If no suspect is identified on the date of initial detection, we may delay filing the SAR for an additional 30 calendar days pending investigation and identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection/confirmation.

We will retain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR. We will make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state regulators, upon proper request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations.

Any employee who is subpoenaed or required to disclose a SAR or the information contained in the SAR, except where disclosure is requested by FinCEN, or other appropriate law enforcement or regulatory agency or an SRO, will decline to produce to the SAR or to provide any information that would disclose that a SAR was prepared or filed. We will notify FinCEN of any such request and our response.

Currency Transaction Reports (CTR)

If we receive currency, we will file with FinCEN CTRs for transactions involving currency that exceed $10,000. Multiple transactions will be treated as a single transaction if they total more than $10,000 during any one business day. We will use the Form CTR at www.fincen.gov/fin104_ctr.pdf.

Note that these are generally not applicable to the way we do business as funds flow through the closing agent, not directly through ResMac, however should a transaction qualify we would report as needed.

8.0 EXCEPTIONS

Exceptions to the policies and procedures promulgated to implement this Program may be approved by Senior Management, so long as such exceptions do not cause the company to violate the AMR requirements.

9.0 ANNUAL REVIEW

This Program shall be revised annually from initial 8/12 implementation by the Compliance Officer and reviewed and approved by Senior Management no less than annually.